ivanti PATCH TUESDAY

Dec. 11, 2018

22 新進漏洞

18 鎖定使用者

3* Zero Days

	漏洞	Critical	Important	鎖定使用者
Adobe	3	3	0	3
Microsoft	17	9	8	13
Mozilla	2	2	0	2

*Released prior to Patch Tuesday

本月份 Microsoft 發布了總共 17 個更新，解決了 39 個獨特的漏洞，其中微軟作業系統更新非常緊迫，Windows 內核中存在令人討厭的零時差漏洞。Adobe 已經解決了 Flash Player 中的兩個零時差漏洞。

	漏洞 Bulletins	CVE 總數量	影響	軟體廠商嚴重等級	Ivanti Priority	威脅風險	Notes	鎖定攻擊	特權管理減輕衝擊
Adobe	*APSB18-44 Flash Player	1	Remote Code Execution	Critical	1	■■■■	*Released November 20th Exploited in Wild: CVE-2018-15981	●	
	*APSB18-42 Flash Player	2	Remote Code Execution	Critical	1	■■■■	*Released December 5th Exploited in Wild: CVE-2018-15982	●	
	APSB18-41 Acrobat and Reader	87	Remote Code Execution	Critical	1	■■■□		●	
Microsoft	*MS18-12-AFP Flash Player	2	Remote Code Execution	Critical	1	■■■■	*Released December 5th Includes Zero Day vulnerabilties CVE-2018-15981, CVE-2018-15982	●	
	MS18-12-EX Exchange Server 2016	1	Tampering	Important	2	■■□□			
	MS18-12-IE Internet Explorer 9, 10, 11	4	Remote Code Execution	Critical	1	■■■□		●	◆
	MS18-12-MR2K8 Server 2008	8	Elevation of Privilege	Important	1	■■■■	Exploited in Wild: CVE-2018-8611	●	
	MS18-12-MR7 Windows 7, Server 2008 R2 and IE	13	Remote Code Execution	Critical	1	■■■■	Exploited in Wild: CVE-2018-8611	●	◆
	MS18-12-MR8 Server 2012 and IE	13	Remote Code Execution	Critical	1	■■■■	Exploited in Wild: CVE-2018-8611	●	◆
	MS18-12-MR81 Windows 8.1, Server 2012 R2 and IE	13	Remote Code Execution	Critical	1	■■■■	Exploited in Wild: CVE-2018-8611	●	◆
	MS18-12-MR81 .NET 3.5-4.7.2	2	Remote Code Execution	Critical	1	■■■□	Publicly Disclosed: CVE-2018-8517		◆
	MS18-12-OFF Excel 2010-2016, Office 2010-2016, Office 2016 and 2019 for macOS, Outlook 2010-2016, PowerPoint 2010-2016	7	Remote Code Execution	Important	2	■■□□		●	◆
	MS18-12-O365 Office 365 ProPlus, Office 2019	6	Remote Code Execution	Important	2				
	MS18-12-SO2K8 Server 2008	8	Elevation of Privilege	Important	1	■■■■	Exploited in Wild: CVE-2018-8611	●	
	MS18-12-SO7 Windows 7 and Server 2008 R2	9	Elevation of Privilege	Important	1		Exploited in Wild: CVE-2018-8611		
	MS18-12-SO8 Server 2012	9	Elevation of Privilege	Important	1	■■■■	Exploited in Wild: CVE-2018-8611	●	
	MS18-12-SO81 Windows 8.1 and Server 2012 R2	9	Remote Code Execution	Critical	1		Exploited in Wild: CVE-2018-8611		
	MS18-12-SONET .NET 3.5-4.7.2	2	Remote Code Execution	Critical	1	■■■□	Publicly Disclosed: CVE-2018-8517		◆
	MS18-12-SPT Sharepoint Server 2010-2019	4	Remote Code Execution	Important	2				
	MS18-12-W10 Windows 10, Server 2016, Server 2019, IE 11, and Edge	23	Remote Code Execution	Critical	1	■■■■	Exploited in Wild: CVE-2018-8611	●	◆
Mozilla	2018-29 Firefox 64	11	Remote Code Execution	Critical	1				
	2018-30 Firefox ESR 60.4	6	Remote Code Execution	Critical	1	■■■□		●	

December Patch Tuesday 2018

微軟本月更新摘要

• Microsoft 發布了總共 17 個更新，解決了 39 個獨特的漏洞。他們解決了一個零時差和一個公開披露的漏洞。受影響的軟體當然包括 Windows、Office、Sharepoint、.Net Framework、Exchange Server 和瀏覽器。之前發布的 IE 還有一個 Flash 更新，請務必進行更新以解決 Adobe 的零時差攻擊。

Microsoft 解決了 Windows 內核中的一個零時差攻擊漏洞（CVE-2018-8611），該漏洞可能允許攻擊者執行特權提升，從而使罪魁禍首能夠在內核模式下運行任意代碼。攻擊者首先必須登錄系統，然後運行經特殊設計的應用程序來控制受影響的系統。從 Windows 7 到 Server 2019 的所有當前支持的 Windows 操作系統中都存在此漏洞。已在舊版操作系統上檢測到漏洞利用，但對於 Windows 10 和 Server 2019，漏洞利用率指數的評級為 1。

Microsoft 已解決.Net Framework（CVE-2018-8517）中一個公開揭露的漏洞，該漏洞可能允許.Net Framework Web 應用程式中的拒絕服務。一旦對易受攻擊的應用程序發出特製請求，無需身份驗證就可以遠端利用此漏洞。可該漏洞被評為重要漏洞，且已被公開揭露，因此提高該漏洞的嚴重等級。

CVE-2018-8626 是個存在於 Windows DNS 伺服器中的漏洞，在無法妥善處理請求時即會造成堆積溢位，並引來遠端程式攻擊，只要是配置成 DNS 伺服器的 Windows 伺服器都受到該漏洞的影響。

CVE-2018-8604 則是因 Exchange Server 未能正確處理檔案資料，當駭客通過 Exchange Server 認證，傳送一個針對特定用戶的惡意請求，就能竄改該名用戶的檔案資料。至於客戶端的 CVE-2018-8631、CVE-2018-8624 與 CVE-2018-8628 則是分別位於 IE、Microsoft Edge 與 PowerPoint 中的遠端程式攻擊漏洞，而且都是很有可能遭到開採的漏洞。

非微軟的本月更新

• Adobe 發布了一個關鍵的 Acrobat 和 Reader 更新，解決了 87 個獨特的漏洞，應盡快更新。 Adobe Flash for Desktop、IE、Chrome 和其他變形都變得緊急關鍵更新，有兩個零日漏洞。Adobe 還在 11 月 20 日和 12 月 5 日發布了 Adobe Flash Player，解決了兩個零時差攻擊漏洞。 11 月 20 日 CVE-2018-15981 在 APSB18-44 中得到解決。駭客會透過製作 Flash .swf 文件來利用此漏洞以安裝惡意軟體。12 月 5 日，另一個 Flash 零時差攻擊（CVE-2018-15982）在 APSB18-42 中得到了解決，該攻擊活動是利用嵌入在 Microsoft Office 檔案中的 ActiveX 來執行。

• Mozilla 發布了 FireFox 和 FireFox ESR 的更新，解決了 11 個獨特的漏洞。Mozilla Firefox 可以解決幾個關鍵漏洞並保證一定的關注，因為瀏覽器是攻擊者易於用戶定位的入口點。

• 1 月份的 Oracle CPU ：請注意 Java SE 8 將於 2019 年 1 月到達公共更新的末日，Java SE 11 是下一個計劃的長期支持版本，2019 年起 Oracle 將針對 Java 更新要求收費。

近期 Patch News

SQLite 爆重大漏洞! 數百萬 App 和 IoT 裝置資料安全拉警報

(來源: ITHome 電腦週報)

廣泛為 App、Chromium 瀏覽器或 IoT 裝置使用的 SQLite 資料庫，存在一項重大漏洞，可能讓駭客遠端執行程式碼。Google 及 SQLite 官方已緊急修補漏洞。基於 SQLite 應用範圍之廣泛，該漏洞可以誘使用戶以瀏覽器造訪特定網頁而遠端觸發，導致程式碼執行、應用程式記憶體洩露或讓 App 當掉。SQLite 官方也已修補了漏洞，並釋出更新版 3.26.0。

微軟網站登入系統有漏洞，用戶點選惡意連結帳號就被綁架

(來源: ITHome 電腦週報)

微軟網站登入系統及驗證漏洞，讓駭客只要發送一則惡意連結，就能輕鬆綁架用戶的微軟服務帳號。這麼一來，駭客即成功繞過 OAuth 驗證而取得有效 token。只要以此交換 session token，即使不知道用戶帳密也能登入帳號。研究人員於 6 月通報微軟這兩個漏洞，微軟已經在 11 月底修補完成。

蘋果更新 iOS 及 macOS 以改善功能並修補漏洞

(來源: ITHome 電腦週報)

蘋果於 12 月初一舉釋出旗下多個系統平臺的更新，包括 iOS 12.1.1、tvOS 12.1.1，Safari 12.0.2 與新版 macOS，其中 iOS 修補了 22 個漏洞，macOS 也修補 15 個漏洞。蘋果並未針對漏洞的嚴重性進行分類，僅公布相關漏洞可能會造成權限擴張、執行任意程式或阻斷服務攻擊。